

Policy #05-02
Date Adopted:
4/6/2005

Blocking of Internet Services
Division of Criminal Justice Services

Approved By:
Francis X. Aumand III
For the VIBRS Advisory
Board

Note: This is a Mandatory Policy.

1. GOALS

1.1. To establish a policy that provides guidance to all users and technical contacts concerning the blocking of internet access at the department level.

1.2. To appropriately manage the risk that various features such as internet access present to the integrity of the network and to the resources on the network.

2. DEFINITIONS

2.1 INTERNET ACCESS – Internet access means the ability to access the internet via the VIBRS network. This means the ability for users to access HTML pages such as Yahoo.com

2.2 INTRANET ACCESS – Intranet access means the ability to access the internal VIBRS network. This means the ability for VIBRS users to access HTML pages such as the VIBRS home page.

2.3 BLOCKING – An automated function that disallows certain events from occurring. Examples: 1.) file sharing can be blocked between sites, 2.) general access to the internet is blocked.

2.4 SUBNET – Every remote local area network on the VIBRS network is allocated the resources to support a set number of IP addressable devices (pcs, printers, etc.). The address resources are not infinite and represent a cost to support.

3. STANDARD / PROCEDURES

3.1 All agencies using the VIBRS network shall have access to the VIBRS homepage, as this is frequently used to notify agencies and their personnel of changes in forms and laws and other law enforcement and informational issues.

3.2 By default, full internet access is automatically granted to all contributing VIBRS agencies. This means that any devices on the agency's subnet can access the internet.

3.2 Internet access is not provided for agencies that are not contributing and using the Spillman software as there CAD/RM system (not entering cases / not doing full NIBRS reporting, etc.). Internet access represents an additional risk to the network and the data on the network. Internet access has to be managed and as such represents a cost in personnel and services.

3.3 As a general rule, with a formal request from an agency, CJS IT staff will block internet access from entire sites or from some portion of the agency's subnet. As an example, if an agency is allowed to have 63 devices on their network, some contiguous range of IP address within the subnet can be blocked. Individual addresses will not be blocked. This represents an effort to give agencies more flexibility in managing their local environment. Local agency support staff will have to decide which group of devices should be connected to the blocked and unblocked ranges.

3.4 Requests for blocking will have to be submitted by agency heads in writing. The requests should be sent to the CJS Help Desk at the Department of Public Safety Headquarters in Waterbury.